09/867,935

Zand, Kambiz

From: PLUS
Sent: Tuesday, March 22, 2005 1:38 PM
To: Zand, Kambiz
Subject: PLUS Results for 09867935

Here are the PLUS search results for 09867935.

This search was prepared by the staff of the Scientific and Technical Information Center, SIRA. If you have questions or comments about this search, please reply via email to PLUS@uspto.gov.


09867935_QUAL.txt


09867935_LIST.txt


09867935_WEST.txt


09867935_EAST.txt


09867935.east


09867935_CLS.txt


09867935_CLSTITLES.txt


09867935_WDS.txt

09867935_CLS
Most Frequently Occurring Classifications of Patents Returned From A Search of 09867935 on March 22, 2005

Original Classifications

8	380/30
2	348/441
2	712/34
2	713/168
2	713/171
2	718/105

Cross-Reference Classifications

6	380/28
4	380/30
3	380/29
3	713/173
2	380/285
2	380/286
2	382/240
2	705/66
2	708/490
2	712/16
2	713/180
2	718/105

Combined Classifications

12	380/30
6	380/28
4	718/105
3	380/285
3	380/29
3	713/173
2	348/441
2	380/286
2	382/240
2	705/66
2	708/490
2	712/11
2	712/15
2	712/16
2	712/21
2	712/34
2	713/168
2	713/169
2	713/171
2	713/180
2	718/100

09867935_CLSTITLES

Titles of Most Frequently Occurring Classifications of Patents Returned

From A Search of 09867935 on March 22, 2005

12 380/30 (8 OR, 4 XR)
Class 380 : CRYPTOGRAPHY
380/28 PARTICULAR ALGORITHMIC FUNCTION ENCODING
380/30 .Public key

6 380/28 (0 OR, 6 XR)
Class 380 : CRYPTOGRAPHY
380/28 PARTICULAR ALGORITHMIC FUNCTION ENCODING

4 718/105 (2 OR, 2 XR)
Class 718 : ELECTRICAL COMPUTERS AND DIGITAL PROCESSING SYSTEMS: VIRTUAL MACHINE TASK OR PROCESS MANAGEMENT OR TASK MANAGEMENT/CONTROL
718/100 TASK MANAGEMENT OR CONTROL
718/102 .Process scheduling
718/105 ..Load balancing

3 380/285 (1 OR, 2 XR)
Class 380 : CRYPTOGRAPHY
380/277 KEY MANAGEMENT
380/278 .Key distribution
380/283 ..User-to-user key distributed over data link (i.e., no center)
380/285 ...By public key method

3 380/29 (0 OR, 3 XR)
Class 380 : CRYPTOGRAPHY
380/28 PARTICULAR ALGORITHMIC FUNCTION ENCODING
380/29 .NBS/DES algorithm

3 713/173 (0 OR, 3 XR)
Class 713 : ELECTRICAL COMPUTERS AND DIGITAL PROCESSING SYSTEMS: SUPPORT
713/150 MULTIPLE COMPUTER COMMUNICATION USING CRYPTOGRAPHY
713/168 .Particular communication authentication technique
713/172 ..Intelligent token
713/173 ...Pre-loaded with certificate

2 348/441 (2 OR, 0 XR)
Class 348 : TELEVISION

348/441 FORMAT CONVERSION

2 380/286 (0 OR, 2 XR)
Class 380 : CRYPTOGRAPHY
380/277 KEY MANAGEMENT
380/286 .Key escrow or recovery

2 382/240 (0 OR, 2 XR)
Class 382 : IMAGE ANALYSIS
382/232 IMAGE COMPRESSION OR CODING
382/240 .Pyramid, hierarchy, or tree structure

2 705/66 (0 OR, 2 XR)
Class 705 : DATA PROCESSING: FINANCIAL, BUSINESS PRACTICE, MANAGEMENT, OR COST/PRICE DETERMINATION
705/50 BUSINESS PROCESSING USING CRYPTOGRAPHY
705/64 .Secure transaction (e.g., EFT/POS)
705/65 ..Including intelligent token (e.g., electronic purse)
705/66 ...Intelligent token initializing or reloading

2 708/490 (0 OR, 2 XR)
Class 708 : ELECTRICAL COMPUTERS: ARITHMETIC PROCESSING AND CALCULATING
708/100 ELECTRICAL DIGITAL CALCULATING COMPUTER
708/200 .Particular function performed
708/490 ..Arithmetical operation

2 712/11 (1 OR, 1 XR)
Class 712 : ELECTRICAL COMPUTERS AND DIGITAL PROCESSING SYSTEMS: PROCESSING ARCHITECTURES AND INSTRUCTION PROCESSING
712/1 PROCESSING ARCHITECTURE
712/10 .Array processor
712/11 ..Array processor element interconnection

2 712/15 (1 OR, 1 XR)
Class 712 : ELECTRICAL COMPUTERS AND DIGITAL PROCESSING SYSTEMS: PROCESSING ARCHITECTURES AND INSTRUCTION PROCESSING
712/1 PROCESSING ARCHITECTURE
712/10 .Array processor
712/11 ..Array processor element interconnection

712/15 ...Reconfiguring

2 712/16 (0 OR, 2 XR)
Class 712 : ELECTRICAL COMPUTERS AND DIGITAL PROCESSING SYSTEMS: PROCESSING ARCHITECTURES AND INSTRUCTION PROCESSING
712/1 PROCESSING ARCHITECTURE
712/10 .Array processor
712/16 ..Array processor operation

2 712/21 (1 OR, 1 XR)
Class 712 : ELECTRICAL COMPUTERS AND DIGITAL PROCESSING SYSTEMS: PROCESSING ARCHITECTURES AND INSTRUCTION PROCESSING
712/1 PROCESSING ARCHITECTURE
712/10 .Array processor
712/16 ..Array processor operation
712/21 ...Multiple instruction, Multiple data (MIMD)

2 712/34 (2 OR, 0 XR)
Class 712 : ELECTRICAL COMPUTERS AND DIGITAL PROCESSING SYSTEMS: PROCESSING ARCHITECTURES AND INSTRUCTION PROCESSING
712/1 PROCESSING ARCHITECTURE
712/32 .Microprocessor or multichip or multimodule processor having sequential program control
712/34 ..Including coprocessor

2 713/168 (2 OR, 0 XR)
Class 713 : ELECTRICAL COMPUTERS AND DIGITAL PROCESSING SYSTEMS: SUPPORT
713/150 MULTIPLE COMPUTER COMMUNICATION USING CRYPTOGRAPHY
713/168 .Particular communication authentication technique

2 713/169 (1 OR, 1 XR)
Class 713 : ELECTRICAL COMPUTERS AND DIGITAL PROCESSING SYSTEMS: SUPPORT
713/150 MULTIPLE COMPUTER COMMUNICATION USING CRYPTOGRAPHY
713/168 .Particular communication authentication technique

713/169 ..Mutual entity authentication

2 713/171 (2 OR, 0 XR)
Class 713 : ELECTRICAL COMPUTERS AND DIGITAL PROCESSING SYSTEMS: SUPPORT
713/150 MULTIPLE COMPUTER COMMUNICATION USING CRYPTOGRAPHY
713/168 .Particular communication authentication technique
713/171 ..Having key exchange

2 713/180 (0 OR, 2 XR)
Class 713 : ELECTRICAL COMPUTERS AND DIGITAL PROCESSING SYSTEMS: SUPPORT
713/150 MULTIPLE COMPUTER COMMUNICATION USING CRYPTOGRAPHY
713/168 .Particular communication authentication technique
713/180 ..Generating specific digital signature type (e.g., blind, shared, or undeniable)

2 718/100 (1 OR, 1 XR)
Class 718 : ELECTRICAL COMPUTERS AND DIGITAL PROCESSING SYSTEMS: VIRTUAL MACHINE TASK OR PROCESS MANAGEMENT OR TASK MANAGEMENT/CONTROL
718/100 TASK MANAGEMENT OR CONTROL

35
PLUS Search Results for S/N 09867935, Searched March 22, 2005

The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present. PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

5819102
5862400
5369708
5524241
5983255
6463457
5539827
6285760
6212277
6212277
5454000
6085210
6085320
6189098
5519778
5638068
6104962
4414624
5630129
5828858
6298430
5668878
5696827
6779111
4939727
5381361
3676661
5568600
5960211
6161180
6243812
5870470
5987131
4860201
6404923

09867935_LIST

3584782
4608659
4979141
5280547
5311454
5365470
6035041
6192388
5539836
5815602
4330833
5503153
5666163
6141054
4920487

~ 9/867,935

Terms used **BLIND SIGNATURE** AND **PERMUTATION** AND **ERROR**

Found **3,286** of **151,219**

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 Strength of two data encryption standard implementations under timing attacks

Alejandro Hevia, Marcos Kiwi

November 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 4

Full text available: pdf(183.73 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We study the vulnerability of two implementations of the Data Encryption Standard (DES) cryptosystem under a timing attack. A timing attack is a method, recently proposed by Paul Kocher, that is designed to break cryptographic systems. It exploits the engineering aspects involved in the implementation of cryptosystems and might succeed even against cryptosystems that remain impervious to sophisticated cryptanalytic techniques. A timing attack is, essentially, a way of obtaining some users ...

Keywords: cryptanalysis, cryptography, data encryption standard, timing attack

2 Signature schemes based on the strong RSA assumption

Ronald Cramer, Victor Shoup

August 2000 **ACM Transactions on Information and System Security (TISSEC)**, Volume 3 Issue 3

Full text available: pdf(168.52 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We describe and analyze a new digital signature scheme. The new scheme is quite efficient, does not require the signer to maintain any state, and can be proven secure against adaptive chosen message attack under a reasonable intractability assumption, the so-called strong RSA assumption. Moreover, a hash function can be incorporated into the scheme in such a way that it is also secure in the random oracle model under the standard RSA assumption.

Keywords: RSA, digital signatures, provable security

3 Practical multi-candidate election system

Olivier Baudron, Pierre-Alain Fouque, David Pointcheval, Jacques Stern, Guillaume Poupard

August 2001 **Proceedings of the twentieth annual ACM symposium on Principles of distributed computing**

h c g e cf c

Full text available: pdf(898.50 KB) Additional Information: full citation, abstract, references, index terms

The aim of electronic voting schemes is to provide a set of protocols that allow voters to cast ballots while a group of authorities collect the votes and output the final tally. In this paper we describe a practical multi-candidate election scheme that guarantees privacy of voters, public verifiability, and robustness against a coalition of malicious authorities. Furthermore, we address the problem of receipt-freeness and incoercibility of voters. Our new scheme is based on the Paillier cryp ...

4 Error spreading: a perception-driven approach to handling error in continuous media streaming

Srivatsan Varadarajan, Hung Q. Ngo, Jaideep Srivastava
February 2002 **IEEE/ACM Transactions on Networking (TON)**, Volume 10 Issue 1

Full text available: pdf(377.04 KB) Additional Information: full citation, abstract, references, citings, index terms

With the growing popularity of the Internet, there is increasing interest in using it for audio and video transmission. Perceptual studies of audio and video viewing have shown that viewers find bursty losses, mostly caused by congestion, to be the most annoying disturbance, and hence these are critical issues to be addressed for continuous media streaming applications. Classical error handling techniques have mostly been geared toward ensuring that the transmission is correct, with no attention ...

Keywords: Bursty error, error spreading, multimedia

5 Coding and Encryption: On error preserving encryption algorithms for wireless video transmission

Ali Saman Saman Tosun, Wu-chi Feng
October 2001 **Proceedings of the ninth ACM international conference on Multimedia**

Full text available: pdf(157.93 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we describe error preserving encryption mechanisms for transmission of vido over wireless networks. One of the main problems with the secure transmission of data over wireless networks is that the bit errors that occur need to typically be sesolved *before* decryption can begin. For vido straming applications, this is unacceptable due to the general requirement that video be presented to the user in a continuous manner with low latency. In this paper, we describe a systematic ...

Keywords: video encryption, wireless video transmission

6 A firmware organization for minimal error evaluation in numerical computations

S. S. Hyder, V. Ung, J. Vignes
September 1974 **Conference record of the 7th annual workshop on Microprogramming**

Full text available: pdf(499.32 KB) Additional Information: full citation, abstract, references, index terms

The use of numerical arithmetic developed for general use in continuous space, on computers where numerical values are represented by a finite number of significant digits leads to errors that tend degenerate as computing progresses. The principle of the permutation-perturbation method is that, while in algebra a given algorithm provides a single result r, the same algorithm carried out on a computer provides a set R of numerical results that are all representative of the exact algebraic re ...

7 Research sessions: compression: Wavelet synopses with error guarantees

Minos Garofalakis, Phillip B. Gibbons

June 2002 **Proceedings of the 2002 ACM SIGMOD international conference on Management of data**

Full text available: pdf(1.44 MB) Additional Information: full citation, abstract, references, citings, index terms

Recent work has demonstrated the effectiveness of the wavelet decomposition in reducing large amounts of data to compact sets of wavelet coefficients (termed "wavelet synopses") that can be used to provide fast and reasonably accurate approximate answers to queries. A major criticism of such techniques is that unlike, for example, random sampling, conventional wavelet synopses do not provide informative error guarantees on the accuracy of individual approximate answers. In fact, as this paper de ...

8 Using permutations in regenerative simulations to reduce variance

James M. Calvin, Marvin K. Nakayama

April 1998 **ACM Transactions on Modeling and Computer Simulation (TOMACS)**, Volume 8 Issue 2

Full text available: pdf(263.12 KB) Additional Information: full citation, abstract, references, citings, index terms

We propose a new estimator for a large class of performance measures obtained from a regenerative simulation of a system having two distinct sequences of regeneration times. To construct our new estimator, we first generate a sample path of a fixed number of cycles based on one sequence of regeneration times, divide the path into segments based on the second sequence of regeneration times, permute the segments, and calculate the performance on the new path using the first sequence of regenerati ...

Keywords: efficiency improvement, permutations, regenerative simulation, variance reduction

9 Session 9: Realizability semantics for error-tolerant logics: preliminary version

John C. Mitchell, Michael J. O'Donnell

March 1986 **Proceedings of the 1986 conference on Theoretical aspects of reasoning about knowledge**

Full text available: pdf(1.59 MB) Additional Information: full citation, abstract, references

Classical and constructive logics have shortcomings as foundations for sophisticated automated reasoning from large amounts of data because a single error in the data could produce a contradiction, logically implying all possible conclusions. Relevance logics have the potential to support sensible reasoning from data that contains a few errors, limiting the impact of those errors to assertions that are naturally related to the erroneous information. There are a number of competing formal syst ...

10 Permutation warping for data parallel volume rendering

Craig M. Wittenbrink, Arun K. Somani

November 1993 **Proceedings of the 1993 symposium on Parallel rendering**

Full text available: pdf(708.10 KB) Additional Information: full citation, references, citings, index terms

11 The computational complexity of recognizing permutation functions

Keju Ma, Joachim von zur Gathen

May 1994 **Proceedings of the twenty-sixth annual ACM symposium on Theory of computing**

Full text available: pdf(867.80 KB) Additional Information: full citation, references, index terms

12 Algorithmic luckiness

Ralf Herbrich, Robert C. Williamson

March 2003 **The Journal of Machine Learning Research**, Volume 3

Full text available: pdf(487.22 KB) Additional Information: full citation, abstract, references, citings, index terms

Classical statistical learning theory studies the generalisation performance of machine learning algorithms rather indirectly. One of the main detours is that algorithms are studied in terms of the hypothesis class that they draw their hypotheses from. In this paper, motivated by the luckiness framework of Shawe-Taylor et al. (1998), we study learning algorithms more directly and in a way that allows us to exploit the serendipity of the training sample. The main difference to previous approaches ...

13 On randomization in sequential and distributed algorithms

Rajiv Gupta, Scott A. Smolka, Shaji Bhaskar

March 1994 **ACM Computing Surveys (CSUR)**, Volume 26 Issue 1

Full text available: pdf(8.01 MB) Additional Information: full citation, abstract, references, citings, index terms

Probabilistic, or randomized, algorithms are fast becoming as commonplace as conventional deterministic algorithms. This survey presents five techniques that have been widely used in the design of randomized algorithms. These techniques are illustrated using 12 randomized algorithms—both sequential and distributed— that span a wide range of applications, including:primality testing (a classical problem in number theory), interactive probabilistic proof s ...

Keywords: Byzantine agreement, CSP, analysis of algorithms, computational complexity, dining philosophers problem, distributed algorithms, graph isomorphism, hashing, interactive probabilistic proof systems, leader election, message routing, nearest-neighbors problem, perfect hashing, primality testing, probabilistic techniques, randomized or probabilistic algorithms, randomized quicksort, sequential algorithms, transitive tournaments, universal hashing

14 The design of MA48: a code for the direct solution of sparse unsymmetric linear systems of equations

I. S. Duff, J. K. Reid

June 1996 **ACM Transactions on Mathematical Software (TOMS)**, Volume 22 Issue 2

Full text available: pdf(464.25 KB) Additional Information: full citation, abstract, references, citings, index terms

We describe the design of a new code for the direct solution of sparse unsymmetric linear systems of equations. The new code utilizes a novel restructuring of the symbolic and numerical phases, which increases speed and saves storage without sacrifice of numerical stability. Other features include switching to full-matrix processing in all phases of the computation enabling the use of all three levels of BLAS, treatment of rectangular or rank-deficient matrices, partial factorization, and i ...

Keywords: BLAS, Gaussian elimination, block triangular form, error estimation, sparse unsymmetric matrices

15 Automatic parsing for content analysis

Frederick J. Damerau

June 1970 **Communications of the ACM**, Volume 13 Issue 6

Full text available: pdf(4.07 MB) Additional Information: full citation, abstract, references, citings

h c g e cf c

Although automatic syntactic and semantic analysis is not yet possible for all of an unrestricted natural language text, some applications, of which content analysis is one, do not have such a stringent coverage requirement. Preliminary studies show that the Harvard Syntactic Analyzer can produce correct and unambiguous identification of the subject and object of certain verbs for approximately half of the relevant occurences. This provides a degree of coverage for content analysis variable ...

Keywords: content analysis, information retrieval, language analysis, natural language processing, parsing, syntactic analysis, text processing

16 Research session 1: award winning papers: From discrepancy to declustering: near-optimal multidimensional declustering strategies for range queries

Chung-Min Chen, Christine T. Cheng

June 2002 **Proceedings of the twenty-first ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems**

Full text available: pdf(214.98 KB) Additional Information: full citation, abstract, references, citings, index terms

Declustering schemes allocate data blocks among multiple disks to enable parallel retrieval. Given a declustering scheme *D,* its *response time* with respect to a query *Q, rt*(*Q*), is defined to be the maximum number of disk blocks of the query stored by the scheme in any one of the disks. If |*Q*| is the number of data blocks in *Q* and *M* is the number of disks then *rt*(*Q*) is at least |*Q*|/*M.* On ...

Keywords: declustering schemes, disk allocations, parallel database, range query

17 From discrepancy to declustering: Near-optimal multidimensional declustering strategies for range queries

Chung-Min Chen, Christine T. Cheng

January 2004 **Journal of the ACM (JACM)**, Volume 51 Issue 1

Full text available: pdf(225.33 KB) Additional Information: full citation, abstract, references, index terms

Declustering schemes allocate data blocks among multiple disks to enable parallel retrieval. Given a declustering scheme *D*, its *response time* with respect to a query *Q*, *rt*(*Q*), is defined to be the maximum number of data blocks of the query stored by the scheme in any one of the disks. If |*Q*| is the number of data blocks in *Q* and *M* is the number of disks, then *rt*(*Q*) is at least □|*Q*|/*M*□. One way to eval ...

Keywords: Declustering schemes, disk allocations, parallel database, range query

18 Computational investigations of low-discrepancy sequences

Ladislav Kocis, William J. Whiten

June 1997 **ACM Transactions on Mathematical Software (TOMS)**, Volume 23 Issue 2

Full text available: pdf(295.58 KB) Additional Information: full citation, abstract, references, citings, index terms

The Halton, Sobol, and Faure sequences and the Braaten-Weller construction of the generalized Halton sequence are studied in order to assess their applicability for the quasi Monte Carlo integration with large number of variates. A modification of the Halton sequence (the Halton sequence leaped) and a new construction of the generalized Halton sequence are suggested for unrestricted number of dimensions and are shown to improve considerably on the original Halton sequence. Problems associat ...

Keywords: Faure sequence, Halton sequence, Monte Carlo and quasi Monte Carlo

integration, Sobol sequence, discrepancy, error of numerical integration, generalized Halton sequence, low-discrepancy sequences

19 On diagnosis and correction of design errors

Irith Pomeranz, Sudhakar M. Reddy

November 1993 **Proceedings of the 1993 IEEE/ACM international conference on Computer-aided design**

Full text available: pdf(981.19 KB) Additional Information: full citation, references, citings

20 A symmetric version of the McEliece public-key cryptosystem

A. Kh. Al Jabri

November 1997 **International Journal of Network Management**, Volume 7 Issue 6

Full text available: pdf(98.33 KB) Additional Information: full citation, abstract, references, index terms

This article exploits the fact that linear codes can correct twice the number of erasures as that of errors, allowing reduction in code size and providing the same level of security. © 1997 John Wiley & Sons, Ltd.

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

h c g e cf c

Results for "(('blind signature')<in>metadata)"
Your search matched **29** of **1137806** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

» View Session History
» New Search

» Key

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

Modify Search

(('blind signature')<in>metadata) >>

Check to search only within this results set

Display Format: (•) Citation ( ) Citation & Abstract

Select Article Information

1. **RSA-based partially blind signature with low computation**
Hung-Yu Chien; Jinn-Ke Jan; Yuh-Min Tseng;
Parallel and Distributed Systems, 2001. ICPADS 2001. Proceedings. Eighth International Conference on
26-29 June 2001 Page(s):385 - 389
AbstractPlus | Full Text: PDF(388 KB) IEEE CNF

2. **A novel blind signature scheme possessed with dual protections**
Jen-Rong Chen, J.; An-Pin Chen; Wen-Mao Lin, R.;
Security Technology, 2003. Proceedings. IEEE 37th Annual 2003 International Carnahan Conference on
14-16 Oct. 2003 Page(s):123 - 127
AbstractPlus | Full Text: PDF(1393 KB) IEEE CNF

3. **A new efficient ID-based proxy blind signature scheme**
Weimin Lang; Yunmeng Tan; Zongkai Yang; Gan Liu; Bing Peng;
Computers and Communications, 2004. Proceedings. ISCC 2004. Ninth International Symposium on
Volume 1, 28 June-1 July 2004 Page(s):407 - 411 Vol.1
AbstractPlus | Full Text: PDF(372 KB) IEEE CNF

4. **Improved user efficient blind signatures**
Zuhua Shao;
Electronics Letters
Volume 36, Issue 16, 3 Aug. 2000 Page(s):1372 - 1374
AbstractPlus | Full Text: PDF(308 KB) IEE JNL

5. **On the robustness of the subspace method for blind signature waveform estimation in asynchronous**
Yunpeng Cheng; Yueming Cai;
Communication Technology Proceedings, 2000. WCC - ICCT 2000. International Conference on
Volume 2, 21-25 Aug. 2000 Page(s):1121 - 1125 vol.2
AbstractPlus | Full Text: PDF(292 KB) IEEE CNF

6. **Fast blind signature waveform tracking under imperfect carrier recovery in DS-CDMA systems**
Zheng Zhao; Qinye Yin; Aigang Feng; Ke Deng;
Vehicular Technology Conference, 2002. VTC Spring 2002. IEEE 55th
Volume 3, 6-9 May 2002 Page(s):1215 - 1218 vol.3
AbstractPlus | Full Text: PDF(370 KB) IEEE CNF

7. **The unlinkability of randomization-enhanced Chaum's blind signature scheme**
Zichen Li;
Parallel and Distributed Processing Symposium, 2003. Proceedings. International
22-26 April 2003 Page(s):5 pp.
AbstractPlus | Full Text: PDF(259 KB) IEEE CNF

8. **ID-based proxy blind signature**
Zheng Dong; Huang Zheng; Kefei Chen; Weidong Kou;
Advanced Information Networking and Applications, 2004. AINA 2004. 18th International Conference on
Volume 2, 29-31 March 2004 Page(s):380 - 383 Vol.2
AbstractPlus | Full Text: PDF(241 KB) IEEE CNF

9. **User efficient blind signatures**
Chun-I Fan; Chin-Laung Lei;
Electronics Letters
Volume 34, Issue 6, 19 March 1998 Page(s):544 - 546
AbstractPlus | Full Text: PDF(416 KB) IEE JNL

10. **Low-computation blind signature schemes based on quadratic residues**
Chun-I Fan; Chin-Laung Lei;
Electronics Letters
Volume 32, Issue 17, 15 Aug. 1996 Page(s):1569 - 1570
AbstractPlus | Full Text: PDF(280 KB) IEE JNL

11. **Efficient blind signature scheme based on quadratic residues**
Fan, C.-I.; Lei, C.-L.;
Electronics Letters
Volume 32, Issue 9, 25 April 1996 Page(s):811 - 813
AbstractPlus | Full Text: PDF(348 KB) IEE JNL

12. **A blind signature scheme based on ElGamal signature**
Mohammed, E.; Emarah, A.E.; El-Shennawy, K.;
EUROCOMM 2000. Information Systems for Enhanced Public Safety and Security. IEEE/AFCEA
17 May 2000 Page(s):51 - 53
AbstractPlus | Full Text: PDF(224 KB) IEEE CNF

13. **A blind signature scheme based on ElGamal signature**
Mohammed, E.; Emarah, A.-E.; El-Shennaway, K.;
Radio Science Conference, 2000. 17th NRSC '2000. Seventeenth National
22-24 Feb. 2000 Page(s):C25/1 - C25/6
AbstractPlus | Full Text: PDF(308 KB) IEEE CNF

14. **An electronic voting scheme based on undeniable blind signature scheme**
Sung-Hyun Yun; Sung-Jin Lee;
Security Technology, 2003. Proceedings. IEEE 37th Annual 2003 International Carnahan Conference on
14-16 Oct. 2003 Page(s):163 - 167
AbstractPlus | Full Text: PDF(1454 KB) IEEE CNF

15. **Comments on Shao's blind signature scheme**
Mingxing He; Pingzhi Fan;
Parallel and Distributed Computing, Applications and Technologies, 2003. PDCAT'2003. Proceedings of the F
Conference on
27-29 Aug. 2003 Page(s):940 - 941
AbstractPlus | Full Text: PDF(209 KB) IEEE CNF

16. **Secure E-voting with blind signature**
Ibrahim, S.; Kamat, M.; Salleh, M.; Aziz, S.R.A.;

Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on
14-15 Jan. 2003 Page(s):193 - 197

AbstractPlus | Full Text: PDF(373 KB) IEEE CNF

☐ **17. The quest for personal control over mobile location privacy**
Qi He; Dapeng Wu; Khosla, P.;
Communications Magazine, IEEE
Volume 42, Issue 5, May 2004 Page(s):130 - 136

AbstractPlus | References | Full Text: PDF(1626 KB) IEEE JNL

☐ **18. Asymptotic performance analysis for signature waveform estimation in synchronous CDMA systems**
Yuen, N.; Friedlander, B.;
Signal Processing, IEEE Transactions on [see also Acoustics, Speech, and Signal Processing, IEEE Transac
Volume 46, Issue 6, June 1998 Page(s):1753 - 1757

AbstractPlus | References | Full Text: PDF(180 KB) IEEE JNL

☐ **19. Cryptanalysis on improved user efficient blind signatures**
Fan, C.-I.; Lei, C.-L.;
Electronics Letters
Volume 37, Issue 10, 10 May 2001 Page(s):630 - 631

AbstractPlus | Full Text: PDF(268 KB) IEE JNL

☐ **20. Cryptanalysis of the blind signatures based on the discrete logarithm problem**
Ham, L.;
Electronics Letters
Volume 31, Issue 14, 6 July 1995 Page(s):1136

AbstractPlus | Full Text: PDF(164 KB) IEE JNL

☐ **21. Performance analysis of signature waveform estimation in synchronous CDMA systems**
Yuen, N.; Friedlander, B.;
Signals, Systems and Computers, 1996. 1996 Conference Record of the Thirtieth Asilomar Conference on
Volume 1, 3-6 Nov. 1996 Page(s):699 - 703 vol.1

AbstractPlus | Full Text: PDF(360 KB) IEEE CNF

☐ **22. The design of protocol for e-voting on the Internet**
Jinn-Ke Jan; Yu-Yi Chen; Yi Lin;
Security Technology, 2001 IEEE 35th International Carnahan Conference on
16-19 Oct. 2001 Page(s):180 - 189

AbstractPlus | Full Text: PDF(492 KB) IEEE CNF

☐ **23. Traceability of double spending in secure electronic cash system**
Hyun Ju Lee; Mun Suk Choi; Chung Sei Rhee;
Computer Networks and Mobile Computing, 2003. ICCNMC 2003. 2003 International Conference on
20-23 Oct. 2003 Page(s):330 - 333

AbstractPlus | Full Text: PDF(799 KB) IEEE CNF

☐ **24. Semi-blind decorrelating multiuser detection for synchronous CDMA**
Wang, S.; Caffery, J., Jr.; Shen, H.;
Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE
Volume 1, 16-20 March 2003 Page(s):379 - 384 vol.1

AbstractPlus | Full Text: PDF(313 KB) IEEE CNF

☐ **25. New key improvements and its application to XTR system**
Xiaofeng Chen; Fei Feng; Yumin Wang;
Advanced Information Networking and Applications, 2003. AINA 2003. 17th International Conference on
27-29 March 2003 Page(s):561 - 564

AbstractPlus | Full Text: PDF(412 KB) IEEE CNF

[redacted]

h eee e eee g e ch e ch e e c e e e